

WHAT IS CLAIMED IS:

1 1. A method of detecting unauthorized actions with respect to encrypted data on a
2 media disk, the media disk including a first portion for pre-recorded content and a second
3 portion for written content, the method comprising:

4 reading an identifier on the media disk, wherein the identifier includes one or more
5 sections located in one of the first portion for pre-recorded content, the second
6 portion for written content, and both the first portion for pre-recorded content
7 and the second portion for written content;

8 determining whether the identifier includes a section located in the second portion
9 written content;

10 comparing the identifier with one or more predetermined types of identifiers for
11 which a section is located in the second portion for written content; and
12 if the identifier is of a type that is one of the one or more predetermined types of
13 identifiers, detecting an unauthorized action.

1 2. The method of claim 1 wherein the reading of the identifier on the media disk is
2 during a media disk access operation including one or more of record, play, get play key,
3 copy, open, close and create.

1 3. The method of claim 2 wherein functionality for the media access disk operation
2 is revoked after detecting the unauthorized action.

1 4. The method of claim 1 wherein the identifier is one of a plurality of identifiers on
2 the media disk, each identifier being associated with one or more files on the media disk, the
3 files including one of pre-recorded content and written content.

1 5. The method of claim 1 wherein the predetermined type is an identifier that
2 indicates pre-recorded content and the identifier relates to a location on the media disk for
3 written content.

4 6. The method of claim 1 wherein the media disk is one of a media disk, a compact
5 disk, a digital video disk, and other digital storage mediums.

1 7. The method of claim 1 wherein the identifier is pre-recorded on the media disk
2 and the media disk is pre-recorded.

1 8. The method of claim 1 wherein the predetermined type is an identifier that
2 indicates written content and the identifier relates to a location on the media disk for the
3 written content that is unique to the media disk.

1 9. The method of claim 1 wherein the identifier is a seed for a key generator, the key
2 generator retrieving one or more keys from a key box, the keys for one or more of unlocking
3 and decrypting files on a media disk.

1 10. The method of claim 1 wherein the identifier is retrieved from a media disk and
2 used in an engine for a validation function, the validation function performing the comparing
3 the identifier with the one or more predetermined types of identifiers and detecting an
4 unauthorized action.

1 11. The method of claim 1 wherein the detection of an unauthorized action results in
2 the validation function providing a failure indication.

1 12. The method of claim 2 wherein detection of an unauthorized action results in
2 revocation of functionality for the media disk access operation.

1 13. The method of claim 1 wherein the method for detecting unauthorized actions
2 occurs when a media disk is accessed by an engine under a digital rights management
3 protocol.

1 14. The method of claim 1 wherein the identifier is located on a media disk
2 coupleable to a host, the host being one of an engine, a device that embeds an engine, a third
3 party digital rights management protocol, an application running in an open computing
4 environment, and a clearinghouse server.

1 15. An apparatus for detecting unauthorized actions with respect to encrypted data on
2 a media disk, the media disk including a first portion for pre-recorded content and a second
3 portion for written content, the apparatus comprising:

4 means for reading an identifier on the media disk, wherein the identifier includes one
5 or more sections located in one of the first portion for pre-recorded content,
6 the second portion for written content, and both the first portion for pre-
7 recorded content and the second portion for written content;

8 means for comparing the identifier with one or more predetermined types of
9 identifiers for which a section located in the second portion for written content
10 is not authorized if the identifier includes a section located in the second
11 portion for written content; and

12 means for detecting an unauthorized action if the identifier is of a type that is one of
13 the one or more predetermined types of identifiers.

1 16. The apparatus of claim 15 further comprising:

2 means for determining whether the identifier is a copy of a pre-recorded identifier or
3 an identifier with the combination of pre-recorded data and written data.

1 17. The apparatus of claim 15 wherein the means for reading of the identifier includes
2 a media disk access component.

1 18. The apparatus of claim 15 wherein the means for reading the identifier operates
2 during an access operation.

1 19. The apparatus of claim 15 wherein the identifier is one of a plurality of identifiers
2 on a media disk, each identifier being associated with one or more files on a media disk, the
3 files including one of pre-recorded content and written content.

1 20. The apparatus of claim 19 wherein at least one of the identifiers is unique to the
2 media disk.

1 21. The apparatus of claim 15 wherein the identifier is a seed for a cryptographic key

2 box, the key box using the identifier to retrieve one or more keys for unlocking files on a

3 media disk.

1 22. An engine configured to detect unauthorized actions with respect to encrypted

2 data on a media disk, the media disk including a first portion for pre-recorded content and a

3 second portion for written content, the engine comprising:

4 a firmware component located on an application specific integrated circuit (ASIC),

5 the firmware component including:

6 a block configured to read an identifier on the media disk, wherein the

7 identifier includes one or more sections located in one of the first

8 portion for pre-recorded content, the second portion for written content

9 and both the first portion for pre-recorded content and the second

10 portion for written content;

11 a block configured to compare the identifier with one or more predetermined

12 types of identifiers for which a section located in the second portion for

13 written content is not authorized if the identifier includes a section

14 located in the second portion for written content; and

15 a block configured to detect an unauthorized action if the identifier is of a type that

16 is one of the one or more predetermined types of identifiers.

1 23. A computer program product, the computer program product comprising:

2 signal bearing media bearing digital information adapted to include programming, the

3 digital information including:

4 a block configured to read an identifier on the media disk, wherein the

5 identifier includes one or more sections located in one of the first

6 portion for pre-recorded content, the second portion for written content

7 and both the first portion for pre-recorded content and the second

8 portion for written content;

9 a block configured to compare the identifier with one or more predetermined

10 types of identifiers for which a section located in the second portion for

11 written content is not authorized if the identifier includes a section
12 located in the second portion for written content; and
13 a block to configured to detect an unauthorized action if the identifier is of a type that
14 is one of the one or more predetermined types of identifiers.

00000000000000000000000000000000